УДК 351.863

С.С. Задворних, *аспірант*
Черкаський державний технологічний університет

ЕКОНОМІЧНА КІБЕРЗЛОЧИННІСТЬ – ГЛОБАЛЬНА ЗАГРОЗА ДЛЯ ЕКОНОМІЧНОЇ СИСТЕМИ УКРАЇНИ

Zadvornykh S.S.
Cherkasy State Technological University

ECONOMIC CYBERCRIME IS A GLOBAL THREAT FOR THE ECONOMIC SYSTEM OF UKRAINE

В статье установлены сущность, уровень и некоторые особенности экономической киберпреступности в Украине на современном этапе, определено актуальность борьбы с этим явлением и установлено наиболее уязвимые с точки зрения киберпреступлений подразделы экономической системы. Также установлены основные риски со стороны киберпреступности для экономики Украины и разработаны рекомендации относительно предотвращения и противодействия экономической киберпреступности на разных уровнях.

Ключевые слова: *аккаунт, кибермошенничество, киберпреступление, теневая экономика, скиминг, интернет-трафик, фаервол, фишерские программы, DdoS-атака.*

The article deals with the nature, level and some particularities of economic cybercrime in present-day Ukraine, the topicality of the fight with this phenomenon has been stated and the most vulnerable from the point of view of cybercrime subdivisions of economic system have been shown. The basic risks of cybercrime for the economy of Ukraine have been analyzed. The recommendations how to avoid and resist economic cybercrime on different levels have been developed.

Key words: *account, cybercrime, cyberfraud*, shadow economy, skimming, internet-traffic, firewall, fisher programmes, DDoS-attack.

Проблема та її зв'язок з науковими та практичними завданнями. Економічна кіберзлочинність набула на сучасному етапі стрімкого поширення. Про актуальність вирішення цієї проблеми свідчить те, що за даними РБК лише за минулий рік через економічну кіберзлочинність світова економіка втратила близько 114 млрд. дол. [3] −це є доказом того, що свідчить про значні збитки для світової економічної систем. З банківських карток українців лише за офіційними даними за минулий рік було знято шахраями близько 116 млн. грн. [6], що свідчить про те, що економічна кіберзлочинність завдає шкоди і вітчизняній економіці.

Аналіз досліджень та публікацій. Окремі аспекти функціонування тіньової економіки з'ясовували у своїх працях: С. Бейкер, Р. Брульхарт – розглядали кримінальний аспект кіберзлочинів та терористичну діяльність кіберзлочинців, Х.-П. Бауер – негативний вплив кіберзлочинності на банківський сектор, більшість досліджень здійснював на замовлення швейцарських банків, І. Баранова у статті «Шахрайство в банківській системі» розглядала окремі аспекти кібершахрайства у банківській сфері, М. Герке – експерт у сфері кіберзлочинності, брав участь у розробці законодавства та заходів по боротьбі з кіберзлочинністю в Європі, у працях «Розуміння кіберзлочинності: Керівництво для країн, що розвиваються» та «Розуміння кіберзлочинності: Явище, завдання та законодавчий аспект» визначив сутність кіберзлочинності та методи боротьби із нею.

Постановка завдання. Мета статті полягає у з'ясуванні рівня економічної кіберзлочинності, найбільш розповсюджених видів шахрайств, пов'язаних із мережею Інтернет в Україні та аналізі заходів, спрямованих на боротьбу з цим явищем з метою отримання досвіду, який можна буде використати в подальшому для боротьби із цим явищем.

Виклад основного матеріалу дослідження. За даними PwC (PricewaterhouseCoopers), кіберзлочинність в Україні належить до п'яти найпоширеніших злочинів поряд із незаконним привласненням майна, корупцією, хабарництвом, недобросовісною конкуренцією та

маніпуляцією із фінансовою звітністю (рис. 1) [9] та, за словами голови СБУ, до головних загроз національної безпеки поряд із посяганням на територіальну цілісність, міжнародним тероризмом та корупцією [1].

Джерело: Україна. Всесвітній огляд економічних злочинів [9, 5]

Рис.1. П'ять найпоширеніших економічних злочинів в Україні та світі в 2011 р.

Про важливість вирішення проблеми кіберзлочинності свідчить також статистика. За даними РБК (РосБізнесКонсалтинг) лише за минулий рік через економічну кіберзлочинність світова економіка втратила близько 114 млрд. дол., у США оцінили збитки від кіберзлочинів за всі роки існування Інтернету в 400 млрд. дол. [3], у 2012 р. через шахрайство з банківськими картками у світі банки недорахувались близько 8 млрд. дол. [2], а в Україні за цей же час 116 млн. грн. [6].

Складність дослідження та боротьби з економічною кіберзлочинністю полягає не лише в тому, що глобальна мережа надає майже необмежені можливості для шахраїв, але й те, що вона виникає не лише в зовнішньому середовищі, але й у внутрішньому як стосовно окремо взятих підприємств чи організацій, так і країни в цілому. Якщо до зовнішніх джерел можуть належати клієнти, постачальники, хакери, конкуренти, то із внутрішніми джерелами все набагато складніше. Тут можна виділити умисне шахрайство та неумисне. До умисного належить так зване інсайдерство. Тобто надання інформації чи несанкціоноване відкриття каналів доступу до неї третім особам працівниками самої компанії з метою отримання особистої вигоди. До найбільш ризикових підрозділів у плані несанкціонованого розповсюдження інформації можна віднести відділ інформаційних технологій, як підрозділ, у якого найповніший доступ до усієї інформації, відділи фінансів та маркетингу як підрозділи, у працівників яких зосереджена стратегічно важлива інформація, юридичний відділ та представників вищого керівництва.

Неумисним шахрайством можна вважати неконтрольований витік інформації, пов'язаний із використанням соціальних мереж, особистої електронної пошти, шпигунських програм, які антивірусна система не змогла виявити та знешкодити. Найбільшу небезпеку становлять соціальні мережі. Вони загрожують не лише проникненням шпигунських, фішерських програм, проте і становлять загрозу в плані соціальної інженерії. Більше ніж у половині організацій (58% в Україні та 60% у світі [9]) не проводять спостереження за використанням соціальних мереж, також у багатьох організаціях відсутній моніторинг інтернет-трафіку. Працівники не лише витрачають робочий час на розваги у мережі, але й створюють загрозу для компанії. Також негативним є той факт, що керівники підприємств зазвичай не надають значення небезпеці, що надходить з боку Інтернету та соціальних мереж. Зі свого боку, регулярні тренінги чи роз'яснювальна робота з приводу кіберзлочинності має позитивний вплив на зниження ненавмисних кіберзлочинів серед персоналу.

Що ж до зовнішніх небезпек з приводу кіберзлочинності, то дослідження показали, що до основних країн походження кіберзлочинності належать Гонконг (разом з Китаєм), Індія, Нігерія, Росія, США, та Україна [9].

Загалом кібератаки за метою спрямування та актуальністю для України можна умовно поділити на п'ять груп:

- Фінансові злочини та шахрайство. Здебільшого здійснюються добре профінансованими групами осіб чи активістами за допомогою сучасних технологій.
- Шпіонаж. Мабуть один із найпоширеніших видів кіберзлочинів. У наш час більшість інформації зберігається в електронному вигляді, здебільшого користувачі активно використовують електронну пошту. Отже, за допомогою сучасних технологій можна перехопити будь-яку інформацію від особистих даних про кожного працівника до інформації про об'єкти інтелектуальної власності та підготовку нових патентів і постраждала сторона не підозрюватиме про втрати.
- Воєнні дії. До цієї групи належать воєнні конфлікти між державами, захоплення стратегічно важливих об'єктів.
- Тероризм. Атаки здійснюються терористичними групами з метою захоплення стратегічно важливих об'єкті.
- Активізм. За своїм характером нагадує усі попередні види, проте дії здійснюються прихильниками ідеалізму [9].

Найбільш розповсюдженими є перші дві групи кіберзлочинів. Якщо компанії частіше зустрічаються із другим видом злочинів, то громадяни із першим.

У побуті для громадян становлять найбільшу небезпеку шахрайства, пов'язані із банківськими картками. Найпростішим способом шахрайства з банкоматами є скімінг, тобто встановлення спеціальних камер на банкоматах, які фіксують інформацію, що вводиться користувачем на клавіатурі, пристроїв-сканерів на гнізда прийому банківських карток, які зчитують із них всю інформацію під час потрапляння картки у банкомат, спеціальних накладок чи альтернативних клавіатур, накладених на основну клавіатуру банкомату, які теж фіксують інформацію, яку користувач вводить у систему. Варто зазначити, що в 2012 р. таких пристроїв на банкоматах було виявлено вдвічі більше, ніж у 2011 – 80 [6]. Серед кіберзлочинів були затримані й іноземці.

На користувачів Інтернету чекає і інша небезпека – перехоплення паролів від електронних платіжних систем та банери, що блокують систему та вимагають переказати певну суму коштів на той чи інший рахунок, інакше погрожують санкціями. Зокрема, минулого року відбулися такі атаки на українських користувачів Інтернету. Здебільшого зловмисники повідомляли про несанкціонований доступ до тих чи інших сайтів або інформації та погрожували кримінальною відповідальністю, блокуванням систем, видаленням всіх даних із комп'ютера у разі несплати штрафу (в середньому від 200 до 1000 гривень). На таких банерах широко використовувалась символіка державних служб України (зокрема МВС, СБУ), що призвело навіть до виникнення послуги розблокування комп'ютерів у фірмах з обслуговування комп'ютерної техніки [5]. Необхідно зазначити, що це не лише завдає шкоди користувачам, але й створює негативну рекламу державним службам, що призводить до підвищення недовіри населення до цих служб.

Негативним є той факт, що Україна увійшла у топ світових джерел DdoS-атак за даними лабораторії Касперського [10] та утримується там вже кілька років. Близько 25% всіх DdoS-атак ((Distributed) Denial-of-service attack – розподілена атака на відмову в обслуговуванні) в 2012 році припадало на Україну (рис. 2), в той час як у 2011 лише 12% [4]. Така статистика має загрозливий характер та свідчить про надто низький захист вітчизняних мереж. Такі атаки завдають шкоду передусім економічній системі країни, оскільки більшість із них спрямована на сайти інтернет-торгівлі (більше чверті), близько 20 та 15% атак відповідно припадає на торгові платформи та ігрові сайти. Також негативним є той факт, що поступово зростає кількість нападів на державні ресурси, зокрема в 2011 р. їх збільшилось на 2% [4]. Це показує вразливість національних систем, призводить до незручностей у користуванні, підриває авторитет владних структур та завдає збитків.

Незважаючи на актуальність проблеми та стратегічну важливість її вирішення, рівень економічної кіберзлочинності в Україні зростає. Це пояснюється не лише відсутністю контролю за соціальними мережами, несприйняттям компаніями загрози, недосконалістю систем захисту, про які вже йшла мова раніше. В Україні немає законодавства, яке би

визначало, що саме є кіберзлочином, в тому числі і економічним кіберзлочином, міру покарання за ці злочини, а також немає розробленої системи протидії та запобігання скоєнню злочинів такого типу, хоч економічні кіберзлочини найчастіше і відносять до тіньової економічної діяльності. Це створює всі можливості для діяльності хакерів на території України.

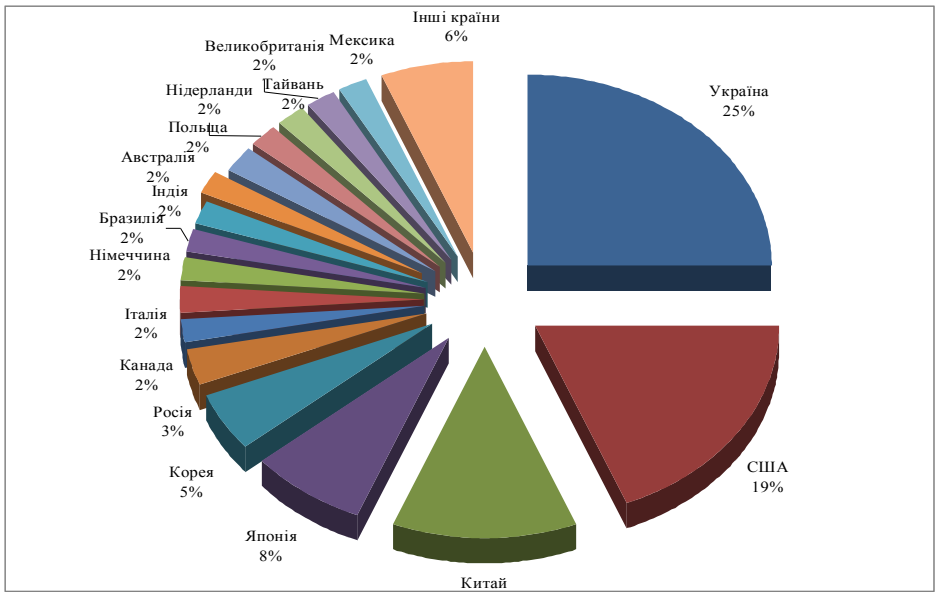

Рис. 2. Розподіл DdoS-атак за країнами

Джерело: DdoS-атаки в первом полугодии 2012 [10]

Позитивним моментом у боротьбі з кіберзлочинністю стало прийняття 7.03.2013 законопроекту «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України». У ньому визначається поняття «кібернетичної безпеки» та «кібернетичного простору» [8]. Якщо зміни буде внесено, це стане першим кроком у визнанні кіберзлочинності, а отже і в боротьбі із кіберзлочинами.

У світовій практиці давно розглядаються кіберзлочини, розроблено законодавство, яке регламентує боротьбу та запобігання таких злочинів. Значною подією у боротьбі з кіберзлочинністю, в тому числі і економічною, стало відкриття 11 грудня 2013 р. в Гаазі в штаб-квартирі Європолу Європейського центру по боротьбі з кіберзлочинністю (ЄС3). Основними напрямами роботи ЄС3 є виявлення незаконної онлайн діяльності, здійснюваної кримінальними угрупуваннями, запобігання та захист від атак, спрямованих на електронні банківські системи, боротьба з онлайн сексуальною експлуатацією дітей, та злочинами, що впливають на інфраструктуру та інформаційну систему ЄС. Захист електронних банківських систем було виокремлено в окремий напрям діяльності ЄС3 після аналізу звітності Європолу, яка проілюструвала, що кіберзлочинці щороку крадуть більше ніж 1,5 млрд. євро з дебетних та кредитних карток [7]. Наскільки дієвою буде діяльність ЄС3 не відомо, проте це суттєвий крок у боротьбі з кіберзлочинністю.

Згідно з виконаним дослідженням ми дійшли висновку, що наслідками економічної кіберзлочинності в Україні є:

– для фізичних осіб як найуразливішої групи – зниження доходів;

– для банків – збитки, зниження довіри вкладників, зростання процентних ставок по кредитах та підняття вартості послуг з метою покриття завданих збитків;

– для держави – формування тіньового бізнесу, зниження довіри до органів державної влади.

– Для боротьби з економічною кіберзлочинністю запропоновано:

для компаній:

– регулярно проводити тренінги та роз'яснювальну роботу серед персоналу з приводу кіберзлочинності;

– підвищити контроль, створити на великих підприємствах чи в організаціях на базі

внутрішньої служби безпеки підрозділ з контролю за ризиковими відділами;

– встановити ефективне антивірусне та антифішерське ліцензійне програмне забезпечення, фаєрволів, здійснювати моніторинг трафіку, блокувати доступ із робочих терміналів до приватних поштових аккаунтів та соціальних мереж, для великих компаній доцільно встановити моноблоки замість стандартних системних блоків;

для банків:

– доцільним є страхування на випадок кібершахрайства;

– як і для компаній, установка надійного програмного забезпечення, заміна стандартних системних блоків на моноблоки;

– створення структурного підрозділу, який би здійснював нагляд за банкоматами та вчасно виявляв скімінг-пристрої. Найкраще залучати по одному спеціалісту у цій галузі до групи інкасаторів кожного разу при обслуговуванні банкомату чи навчити інкасаторів виявляти такі пристрої;

– доцільно, використовуючи європейський досвід, здійснити перехід до чіпованих карток, що б значно ускладнило роботу шахраїв та слугувало б додатковим захистом користувачів;

– налагодити систему розпізнавання власників карток та провадити регулярний запис із камер спостереження на банкоматах, що допомогло б знизити рівень шахрайства та допомогти у проведенні розслідувань за фактом крадіжки коштів із карток;

для держави:

– прийняти запропоновані зміни до законодавства, що дало б змогу визнати економічну кіберзлочинність та встановити міри покарання;

– створити підрозділ по боротьбі з кіберзлочинністю;

– розробити власну захищену операційну систему із закритим кодом, яка була б єдиною та обов'язковою для всіх державних структур, що допомогло би запобігти ненавмисний витік інформації та значну частину кібератак.

Висновки. Економічна кіберзлочинність на сучасному етапі набула значного поширення як в Україні, так і за кордоном, ставши явищем планетарного масштабу. Подолання економічної кіберзлочинності є пріоритетним напрямом економічної політики України. Для подолання цього явища необхідно детально дослідити всі його аспекти та розробити законодавчу базу, яка б визначала сутність кіберзлочину та передбачала міру покарання за злочини, класифіковані як кібернетичні.

У подальших дослідженнях доцільніше сконцентрувати увагу на дослідженні характерних особливостей економічної кіберзлочинності саме для України, простежити динаміку розвитку кожного із напрямів кіберзлочинності, оскільки рівень економічної кіберзлочинності в Україні один із найвищих, а такий аналіз дасть змогу детально дослідити це явище, що було б корисним при розробці законодавства та заходів по боротьбі з економічною кіберзлочинністю в Україні.

Список літератури

1. Економічна правда [Електронний ресурс]. – Режим доступу: http://www.epravda.com.ua/news/2012/03/23/319485/
2. Економічна правда [Електронний ресурс]. – Режим доступу: http://www.epravda.com.ua/columns/2013/02/14/361566/
3. Корреспондент [Електронний ресурс]. – Режим доступу: http://ua.korrespondent.net/business/web/1326100-kiberzlochinnist-koshtue-svitovij-ekonomici-114-mlrd-na-rik
4. Корреспондент [Електронний ресурс]. – Режим доступу: http://ua.korrespondent.net/business/web/1322313-ukrayina-uvijshla-u-top-svitovih-dzherel-ddos-atak-laboratoriya-kasperskogo
5. Срочная помощь компъютеру [Електронний ресурс]. – Режим доступу: http://pk03.com.ua/article-56.html
6. ТСН [Електронний ресурс]. – Режим доступу: http://tsn.ua/groshi/kiberzlochinci-spustoshuyut-rahunki-ukrayinciv-viduryuyuchi-v-interneti-yih-bankivski-dani-280297.html

7. Украинские национальные новости [Електронний ресурс]. – Режим доступу: http://www.unn.com.ua/ru/news/1175980−yevropeyskiy−tsentr−po−borotbi−z−kiberzlochinnisty−vidkriyetsya−11−sichnya−u−gaazi%20
8. Урядовий портал [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/uk/publish/article?art_id=246124630&cat_id=244276429
9. PwC [Електронний ресурс]. – Режим доступу: http://www.pwc.com/uk_UA/ua/press−room/assets/GECS_Ukraine_ua.pdf
10. Securelist [Електронний ресурс]. – Режим доступу: http://www.securelist.com/ru/blog/207764220/DDoS_ataki_v_pervom_polugodii_2012

Стаття надійшла до редакції 04.03.2013